REMARKS/ARGUMENTS

The Applicant acknowledges, with thanks, the office action dated April 15, 2009. Claims 1-16, 26, and 28 are currently pending. Claims 1 and 9 have been amended and claim 29-30 are new. No new matter has been added. Hashing the result keys for both the server and the peer and comparing the two hashes is disclosed in previously presented claim 26 and paragraph 33 of the original specification. Selecting an alternate asymmetric encryption algorithm responsive to detecting a man-in-the-middle attack is disclosed in paragraph 59 of the original specification. A Diffie-Helman key exchange being either server-authenticated or anonymous is disclosed in paragraph 57 of the original specification. Reconsideration of this application as currently amended is respectfully requested.

Prior-Art Matters

Claims 1-16, 26, and 28 were rejected under 35 U.S.C. §103(a) as being unpatentable over Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40 (*hereinafter*, "Funk") in view of U.S. Patent Application Publication No. 2002/0002613 to Freeman et al. (*hereinafter,* "Freeman"). Withdrawal of these rejections is requested for the reasons set forth herein.

Independent claim 1, as currently amended, recites a method of secure communication. A secure tunnel is established between a server and a peer using an encryption algorithm that establishes an encryption key. The peer is authenticated with the server over the secured tunnel establishing an authentication key. The server encryption and authentication keys are hashed to produce a first hash and the peer encryption and authentication keys are hashed to produce a second hash. The two hashes are compared to verify that the server and the peer possess the same encryption and authentication keys. Network access credentials are provisioned to the peer using the secured tunnel responsive to verifying the peer possesses the same encryption and authentication keys as the server. An authorization failure is signaled to the peer upon conclusion of the provisioning of the network access credentials, prior to the peer authenticating using the provisioned credentials, and the peer is denied access to the network by the server until

the peer authenticates using the provisioned credentials. Independent claim 9 recites an implementation of claim 1.

By contrast, Funk uses EAP-TTLS to gain access to the network. TLS is used to authenticate the client with the server. Once a successful authentication has occurred, the TLS layer is used to securely tunnel information between the client and the server. However, Funk does not teach hashing a server encryption key and a server authentication key to produce a first hash, hashing a peer encryption key and a peer authentication key to produce a second hash, and comparing the two hashes to verify the server and the peer possess the same encryption and authentication keys.

The Office Action relies on Funk's discussion of using a master secret and random values established during the handshake to establish authentication when a challenge-based authentication mechanism is used (page 5). The Office Action also relies on Funk's discussion of verifying the value of a challenge response by comparing it to a value generated as challenge material (page 5). However, this discussion by Funk refers to the process of authenticating using a challenge response mechanism such as MS-CHAP-V2. Funk says nothing about taking the results of the MS-CHAP-V2 process (the server's authentication key) and hashing it with the server's encryption key, which was generated as a result of establishing the secure tunnel, and then comparing it to a hash of the client's authentication key and encryption key. This comparison of the hash values provides an extra guard against man-in-the-middle attacks.

Additionally, as stated in the Office Action, Funk is silent on signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisional credentials, and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials.

The aforementioned deficiencies in Funk are not remedied by the teachings of Freeman. Freeman teaches a method and apparatus for communicating among a network of servers. A server has a first plurality of subsystems and a first event bus associated with the first plurality of subsystems. The first event bus includes a first event delivery object having a first dispatch table and a first transport mechanism associated with the first event delivery object. A second server has a second plurality of subsystems. One of the first plurality of subsystems communicates with one of the second plurality of subsystems by transmitting an event to the first transport mechanism based on an entry in the first dispatch table. However, Freeman does not teach or

suggest hashing a server encryption key and a server authentication key to produce a first hash, hashing a peer encryption key and a peer authentication key to produce a second hash, and comparing the two hashes to verify the server and the peer possess the same encryption and authentication keys.

Freeman is relied on by the Office Action to teach signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisional credentials, and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials (page 3). Applicant respectfully disagrees with this interpretation of Freeman. Freeman teaches signaling a failed provisioning of authentication credentials (¶515). However, Freeman does not teach or suggest signaling an authorization failure upon successful provisioning of authentication credentials, prior to the peer authenticating using the provisioned authentication credentials as is taught in claim 1. This helps to increase security and to prevent third party attacks by ensuring that parties ensue in actual authentication versus a provisioning protocol. Thus, neither Funk nor Freeman, alone or in combination, teach or suggest each and every element of independent claims 1 and 9. Therefore, for the reasons set forth, withdrawal of this rejection is respectfully requested.

Claims 2-8 and 28 depend directly from claim 1 and therefore contain each and every element of claim 1. Claims 10-16 depend directly from claim 9 and therefore contain each and every element of claim 9. Therefore, for the same reasons already set forth for claims 1 and 9, withdrawal of rejections of claims 2-8, 10-16, and 28 is respectfully requested.

In addition, claim 29 recites the method of claim 5 further comprising selecting an alternate asymmetric encryption algorithm after detecting a man-in-the-middle attack. Using Diffie-Hellman key exchange as the asymmetric encryption algorithm presents a viable option as there may be deployments that are more confined and willing to accept the risk of a man-in-the-middle attack in exchange for ease of use. However, a more secure encryption algorithm may be desired in response to detecting a man-in-the-middle attack. Neither Funk nor Freeman teach or suggest the flexibility of detecting a man-in-the-middle attack and selecting an alternate encryption algorithm in response. Thus, in addition to the reasons already set forth, claim 29 is not anticipated and/or obvious in view of Funk or Freeman.

Conclusion

Withdrawal of these rejections is requested for the reasons set forth and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: 7-10-09

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009